Six Point Cyber Security Check List for Company Directors and Board Members

1. Has your organisation implemented the Australian Signals Directorate's Top 4 Cyber Risk Mitigation Strategies?

   The Australian Signals Directorate (**ASD**) suggests that implementing ASD's ***Top four mitigation strategies to protect your ICT system*** can address up to 85% of targeted cyber intrusions.

2. Ask your CIO the Cyber Security Operations Centre's ***Questions Senior Management Need to be Asking about Cyber Security:***

   a) What would a serious cyber incident cost our organisation?
   b) Who would benefit from having access to our information?
   c) What makes us secure against threats?
   d) Is the behaviour of our staff enabling a strong security culture?
   e) Are we ready to respond to a cyber security incident?
   f) Have we applied ASD's top four mitigation strategies?

3. **Take the ASIC "Cyber Resilience Health Check"**

   ASIC's ***Cyber Resilience: Health Check (ASIC Report 429)*** contains a number of "Health Check Prompts" and provides useful guidance as to the questions directors and officers can ask in assessing their organisation's awareness of and preparedness for cyber security issues.

4. **Does your organisation collect or handle personal information? If so is it compliant with the *Privacy Act 1988* (Cth)?**

   Does your organisation meet the legal requirement to *take such steps as are reasonable in the circumstances* to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure (Australian Privacy Principle (**APP**) no. 11)?

5. **Does your organisation process card payments?**

   If so, is it (or its card payment processing service provider) compliant with the Payment Card Industry's *Data Security Standard (DSS): Requirements and Security Assessment Procedures*?

6. **Are your organisation and its outsourced services/service providers compliant with applicable industry standards? Are third party products used in your organisation compliant?**

   For example, the ISO 27000 series of IT and cyber security standards published by the International Organisation for Standardisation and the International Electrotechnical Commission. See ISO/IEC 27018:2014; ISO/IEC 27001:2015.

Sean Field, Special Counsel, Maddocks